# RANCANGAN KRIPTOGRAFI *HYBRID* KOMBINASI METODE VIGENERE CIPHER DAN ELGAMAL PADA PENGAMANAN PESAN RAHASIA

*Bella Ariska [1)], Suroso [2)], Jon Endri [3)]*

*[1),2),3 )]Program Studi Teknik Telekomunikasi Jurusan Teknik Elektro, Politeknik Negeri Sriwijaya Palembang*
*Jl. Srijaya Negara Bukit Besar, Ilir Barat 1 Kota Palembang*
*Email : bellaariska10@yahoo.com*

**Abstrak.** *Pada paper ini dibuat suatu penjelasan terhadap rancangan dan uraian dari setiap proses enkripsi dan dekripsi untuk keamanan dalam pengiriman informasi pesan rahasia. Pada paper ini digunakan kombinasi dua metode yaitu Vigenere Cipher dan ElGamal. Metode Vigenere Cipher menggunakan kunci yang sama untuk proses enkripsi dan dekripsi. Sedangkan ElGamal menggunakan dua kunci yang berbeda yaitu kunci rahasia dan kunci publik untuk proses enkripsi dan dekripsi. Kombinasi dua metode ini disebut kriptografi hibrid yang memiliki keunggulan dalam kecepatan pemrosesan data tanpa mengurangi kenyamanan dan keamanan. Pada paper ini memanfaatkan dua tingkatan kunci yang artinya proses enkripsi dan dekripsi dilakukan masing-masing dua kali penguncian. Untuk proses enkripsi digunakan kunci publik, sedangkan untuk proses dekripsi digunakan kunci rahasia dan kunci publik. Proses pembentukan kunci ini dibentuk oleh penerima menggunakan ElGamal yang menghasilkan kunci rahasia dan kunci publik. Kemudian penerima akan memberikan hasil kunci publik kepada pengirim untuk dilakukan proses enkripsi, dan penerima tetap menjaga kerahasiaan kunci rahasia untuk digunakan pada proses dekripsi dari pesan yang telah diterima dari pengirim.*

**Kata kunci :** *Vigenere Cipher, ElGamal, Enkripsi, Dekripsi*

## 1. Pendahuluan

Dalam perkembangan teknologi saat ini informasi sangat rentan terhadap serangan dan gangguan dari pihak lain. Saat pengirim dan penerima bertukar informasi melalui SMS, Email atau jenis chatting lainnya, lalu lintas informasi tersebut tidaklah terjamin keamanannya contohnya serangan *man in the middle*, seseorang dapat membaca, menyisipkan, ataupun mengubah data antara dua pihak yang sedang bertukar informasi atau berkomunikasi, seseorang tersebut menempatkan dirinya di tengah pembicaraan dan menyamar sebagai orang lain (M. Mustari, 2010) . Dalam bidang industri pastinya diperlukan sistem pengamanan dalam pengiriman data atau informasi berupa pesan teks yang bersifat rahasia, akan dapat menimbulkan kerugian bagi pemilik informasi apabila informasi tersebut diketahui oleh pihak lain karena tidak semua data atau informasi dapat diketahui oleh pihak lain (bersifat publik) yang artinya informasi tersebut bersifat rahasia. Atas dasar kesadaran inilah maka perlu adanya tindakan dalam pengamanan informasi tersebut. Keamanan suatu informasi merupakan salah satu prioritas yang sangat utama bagi berbagai bidang dan perseorangan, terkhususnya bagi perusahaan, periklanan, perindustrian apabalagi yang sedang dalam proses *development.*

Salah satu teknik pengamanan dalam penyampaian informasi adalah dengan melakukan enkripsi dan dekripsi terhadap informasi tersebut, yang dikenal dengan teknik kriptografi. Kritografi adalah ilmu seni untuk menjaga kerahasian dan keamanan suatu data atau informasi ketika informasi dikirim dari suatu tempat ke tempat yang lain (Ariyus, 2008). Prinsip dasar pengamanan kriptografi adalah proses enkripsi dan dekripsi.

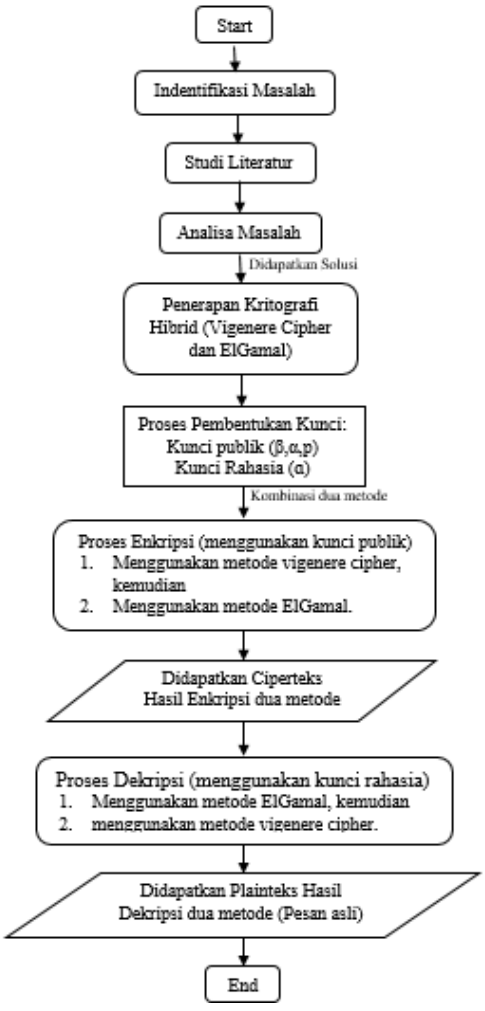
Proses enkripsi adalah sebuah proses penyandian yang melakukan perubahan sebuah kode (pesan) dari yang bisa dimengerti (plainteks) menjadi sebuah kode yang tidak bisa dimengerti (cipherteks). Sedangkan proses dekripsi adalah kebalikan untuk mengubah cipherteks menjadi plainteks (Massandy, 2009). Ada dua macam kriptografi yaitu algoritma simetris (*symmetric algorithms*) dan algoritma asimetris (*asymmetric algorithms*). Algoritma simetris disebut dengan algoritma kunci rahasia adalah algoritma yang menggunakan kunci yang sama untuk enkripsi dan dekripsinya. Sedangkan algoritma asimetris disebut dengan algoritma kunci publik, menggunakan dua jenis kunci kriptografi yaitu kunci publik (*public* key) dan kunci rahasia (*secret key*) (Ariyus, 2008).

Ada beberapa penelitian yang telah dilakukan seperti pada metode vigenere cipher. Salah satunya adalah "Enkripsi Data Berupa Teks Menggunakan Metode Modifikasi Vigenere Cipher". Pada penelitian ini enkripsi menggunakan metode modifikasi vigenere cipher, disimpulkan bawa metode tersebut lebih aman dibandingkan dengan metode vigenere cipher yang telah ada. Disebabkan metode modifikasi vigenere cipher tidak memiliki pengulangan kata pada sandi yang dihasilkan (Ifanto, 2009). Adapun penelitian yang berkaitan dengan algoritma ElGamal adalah "Metode Enkripsi dan Dekripsi dengan menggunakan Algoritma ElGamal". Dalam penelitian ini diperoleh bahwa menggunakan algoritma ElGamal keamanannya terletak pada logaritma diskrit pada grup pengandaan bilangan bulat modulo prima, dengan mengambil nilai bilangan prima yang besar, maka upaya pemecahan pesan akan sangat sungkar dilakukan (Massandy, 2009).

Dalam permasalahan keamanan ini penulis mengkombinasikan dua metode keamanan untuk menjaga kerahasiaan pesan pada saat pengiriman SMS atau jenis chatting lainnya dengan menggunakan teknik kriptografi hibrid. Kriptografi hibrid merupakan penggabungan antara dua algoritma simetris dan asimetris. Metode yang digunakan yaitu Vigenere Cipher dan ElGamal. Metode Vigenere Cipher merupakan golongan simetris dan ElGamal merupakan golongan asimetris. Pada paper ini berisi rancangan atau uraian proses pembentukan kunci, proses enkripsi dan proses dekripsi dalam pengamanan pesan menggunakan dua metode tersebut.

### 1.1 Metodelogi

Penelitian ini dilakukan secara bertahap sesuai dengan kerangka yang terdapat pada alur diagram berikut.




Gambar 1. Flowchart Alur Penelitian

1) Identifikasi Masalah

Merupakan tahapan observasi pada peristiwa pertukaran informasi berbentuk SMS dan atau Chatting. Fokus pengamatan terletak pada masalah keamanan dari pertukaran informasi itu sendiri. Tujuan observasi ini adalah untuk mengidentifikasi masalah secara tepat mewakili permasalahan yang sedang berkembang.

2) Studi Literatur

Merupakan tahap pengumpulan materi dari berbagai buku referensi dan jurnal-jurnal nasional yang sesuai dengan topik permasalahan yang sedang dikembangkan yaitu penggunaan kriptogrfi *hybrid* menggunakan metode Vigenere Cipher dan ElGamal pada pengamanan pesan rahasia berbentuk SMS dan atau Chatting.

3) Analisa Masalah

Pada tahap ini, dilakukan analisa terhadap permasalahan keamanan pada pertukaran informasi via SMS dan atau Chatting. Analisa ini mengasumsikan baik pengirim dan penerima tidak menyadari bahwa informasi yang dikirimkan benar-benar aman dan terjaga kerahasiaannya. Solusi yang ditawarkan adalah dengan melakukan proses enkripsi dan deskripsi menggunakan teknik kriftograpi *hybrid* dengan kombinasi dua metode yaitu Vigenere Cipher dan ElGamal.

## 1.2 Tinjauan Pustaka

1) Vigenere Cipher

Vigenere Cipher adalah suatu algoritma kriptografi klasik dengan teknik substitusi yang ditemukan oleh Giovan Battista Bellaso. Beliau menuliskan metodenya tersebut pada bukunya yang berjudul La Cifra del. Sig. Giovan Battista Bellaso pada tahun 1553. Nama Vigenere sendiri diambil dari seorang yang bernama Blaise de Vigenere. Vigenere Cipher menggunakan suatu kunci yang memiliki panjang kunci tertentu (Noercholis & Asyanto, 2014)

Vigenere Cipher ini adalah suatu metode yang dirancang untuk memperbaiki kelemahan dari algoritma subtitusi tunggal. Vigenere cipher merupakan teknik kriptografi sederhana yang lebih aman. Dikembangkan dari metode caesar cipher, metode ini menggunakan karakter huruf sebagai kunci enkripsi. Vigenere cipher juga merupakan polyalphabetic substition cipher (Prabowo & Hangga, 2015). Berikut ini inisial karakter metode Vigenere Cipher pada Tabel 1 berikut (Putra, 2017).

Tabel 1. Inisial Karakter Vigenere Cipher

| a | b | c | d | e | f | g | h | I | j | k | L | m | N |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 |
| o | p | q | r | s | t | u | v | w | x | y | Z | A | B |
| 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 |
| C | D | E | F | G | H | I | J | K | L | M | N | O | P |
| 28 | 29 | 30 | 31 | 32 | 33 | 34 | 35 | 36 | 37 | 38 | 39 | 40 | 41 |
| Q | R | S | T | U | V | W | X | Y | Z | 0 | 1 | 2 | 3 |
| 42 | 43 | 44 | 45 | 46 | 47 | 48 | 49 | 50 | 51 | 52 | 53 | 54 | 55 |
| 4 | 5 | 6 | 7 | 8 | 9 | ‘ | ~ | ! | @ | # | $ | % | ^ |
| 56 | 57 | 58 | 59 | 60 | 61 | 62 | 63 | 64 | 65 | 66 | 67 | 68 | 69 |
| & | * | ( | ) | _ | - | = | + | { | } | [ | ] | \| | ; |
| 70 | 71 | 72 | 73 | 74 | 75 | 76 | 77 | 78 | 79 | 80 | 81 | 82 | 83 |
| : | “ | < | > | , | . | ? | / | | | | | | |
| 84 | 85 | 86 | 87 | 88 | 89 | 90 | 91 | 92 | | | | | |

Pada vigenere cipher, kunci yang digunakan berupa karakter yang dimasukan oleh pengguna. Karakter yang digunakan pada vigenere cipher disini yaitu a, b, c, ..., z, A, B, C, ..., Z, 0, 1, 2, 3, ..., 9, dan

karakter simbol lainnya seperti pada Tabel 1 tersebut. Proses enkripsi dimulai dengan menyesuaikan setiap huruf dengan angka 0 sampai 92. Dan hasil enkripsi didapatkan dari menambahkan nilai pesan dengan kunci. Hasil akan dikurangi 93 apabila nilai hasil lebih dari 92. Model matematis algoritma enkripsi vigenere cipher dapat dihitung dengan menggunakan persamaan (1):

$$E_i = (P_i + K_i) \bmod 93 \quad (1)$$

Keterangan :

$E_i$ = Enkripsi karakter i
$P_i$ = Karakter pada pesan
$K_i$ = karakter pada kunci i

Sedangkan algoritma dekripsi vigenere cipher dapat diketahui dengan menggunakan persamaan (2):

$$D_i = (C_i - K_i) \bmod 93 \quad (2)$$

Keterangan :

$D_i$ = Dekripsi karakter i
$K_i$= karakter pada kunci
$C_i$ = karakter pada cipherteks

2) ElGamal

ElGamal adalah suatu *public key cryptosystem* asimetris yang dibuat pada tahun 1985 oleh Taher ElGamal. ElGamal digunakan untuk melakukan enkripsi dan tanda tangan digital. ElGamal menggunakan analisis matematis dalam enkripsinya yang didasarkan pada masalah logaritma diskrit. ElGamal terdiri dari tiga proses, yaitu proses pembentukan kunci, proses enkripsi dan proses dekripsi. Algoritma ini merupakan cipher blok, yaitu melakukan proses enkripsi pada blok-blok plainteks dan menghasilkan blok-blok cipherteks yang kemudian dilakukan proses dekripsi, dan hasilnya digabungkan kembali menjadi pesan yang utuh dan dapat dimengerti. Untuk membentuk sistem kriptografi ElGamal, dibutuhkan bilangan prima p dan elemen primitif α.

Dalam ElGamal menggunakan bilangan bulat dalam proses perhitungannya, maka pesan harus dikonversi ke dalam suatu bilangan bulat. Untuk mengubah pesan menjadi bilangan bulat digunakan kode ASCII (*American Standard for Information Interchange*). Kode ASCII merupakan representasi numerik dari karakter-karakter yang digunakan pada komputer, serta mempunyai nilai minimal 0 dan maksimal 255. Oleh karena itu, berdasarkan sistem kriptografi ElGamal di atas maka harus digunakan bilangan prima yang lebih besar dari 255 (Nasional, Mada, Matematika, Ilmu, & Alam, 2007).

- Pembentukan Kunci

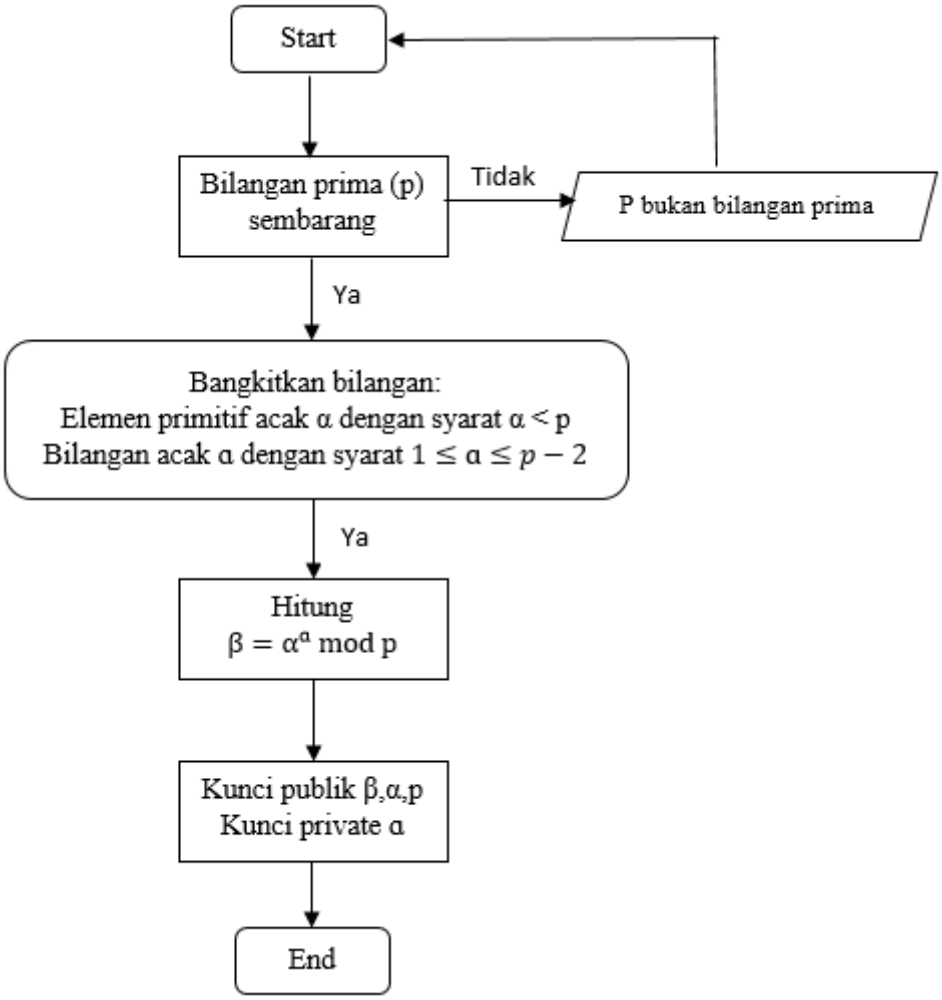
Pada proses pembentukan kunci ElGamal terdiri dari kunci rahasia dan kunci publik yang termasuk dalam golongan algoritma asimetris. Proses pembentukan kunci ini merupakan proses penentuan suatu bilangan yang kemudian akan digunakan sebagai kunci pada proses enkripsi dan dekripsi pesan.

Pada proses ini dibutuhkan bilangan prima *p*, elemen primitif acak $\alpha$ dan bilangan sembarang α. Kunci publik untuk enkripsi berupa pasangan 3 bilangan yang dibangkitkan dari nilai (p, $\alpha, \beta$), dengan

$$\beta = \alpha^a \bmod p \quad (3)$$

Sedangkan kunci rahasia untuk dekripsi terdiri dari nilai α, p. Masing-masing nilai mempunyai persyaratan yang harus dipenuhi. Langkah-langkah dalam pembuatan kunci adalah sebagai berikut :
1. Pilih sembarang bilangan prima p, dengan syarat p > 255.
2. Pilih elemen primitif acak $\alpha$ dengan syarat $\alpha$ < p.

3. Pilih bilangan acak α dengan syarat $1 \leq \alpha \leq p - 2$.
4. Hitung $\beta = \alpha^a \bmod p$
5. Publikasikan nilai *p*, *α dan β,* serta rahasiakan nilai *a*.




Gambar 2. Flowchart Proses Pembentukan Kunci

Pihak yang membuat kunci publik dan kunci rahasia adalah penerima, sedangkan pihak pengirim hanya mengetahui kunci publik yang diberikan oleh penerima, dan kunci publik tersebut digunakan untuk mengenkripsi pesan. Jadi keuntungan menggunakan algoritma kriptografi kunci publik adalah tidak ada permasalahan pada distribusi kunci apabila jumlah pengirim sangat banyak serta tidak ada kepastian keamnan jalur yang digunakan (Massandy, 2009).

- Enkripsi

Proses enkripsi merupakan proses mengubah pesan asli (plainteks) menjadi pesan rahasia (chiperteks). Pada proses ini digunakan kunci publik ($p$,$\alpha$, $\beta$). Langkah-langkah dalam mengenkripsi pesan adalah sebagai berikut :

1. Potong plainteks menjadi blok-blok $m_1$, $m_2$, $m_3$, …, $m_n$ nilai setiap blok di dalam selang [0, p – 1].
2. Ubah nilai blok pesan ke dalam nilai ASCII.
3. Pilih bilangan acak k, dengan syarat $1 \leq k \leq p - 1$ sebanyak m.
4. Setiap blok m dienkripsi dengan rumus sebagai berikut :

$$\gamma = \alpha^{ki} \bmod p \quad \text{.....(4)}$$

$$\delta = \beta^{ki} \, m \bmod p \quad \text{.....(5)}$$

Susun chiperteks dengan urutan $\gamma_1, \delta_1, \gamma_2, \delta_2, \ldots, \gamma_n, \delta_n$. Pasangan γ dan δ adalah chiperteks untuk blok pesan m.

- Dekripsi

Proses dekripsi merupakan proses mengubah pesan rahasia (chiperteks) menjadi pesan asli (plainteks). Pada proses ini digunakan kunci pribadi (α, *p*). Langkah-langkah dalam mendekripsi pesan adalah sebagai berikut :

1. Hitung plaintext m dengan persamaan (6) sebagai berikut
$$m_i = \delta_i . \gamma_i^{(p-1-\alpha)} \bmod p \quad \text{.....(6)}$$
2. Nilai $m_i$ yang di dapat dalam bentuk ASCII kemudian diubah menjadi plainteks
3. Susun plainteks dengan urutan $m_1, m_2, m_3, \ldots, m_n$.

Hasil yang didapat dari proses dekripsi berupa pesan asli (plainteks).

**2. Pembahasan**

Diberikan contoh kasus kombinasi dua metode yaitu vigenere cipher dan ElGamal dalam pengeiriman pesan rahasia. Misalkan Alice ingin memberikan informasi kepada temannya Bob. Alice memberitahukan tempat lokasi keberadaannya kepada Bob, akan tetapi pesan harus dirahasiakan. Pesan yang akan diberitahukan kepada Bob adalah "Perpustakaan".

A. Proses Pemebentukan Kunci

Untuk melakukan enkripsi pesan lakukan pembentukan kunci, proses pembentukan kunci dibentuk menggunakan ElGamal sebagai berikut:

- ✓ Pembentukan Kunci
  Pada metode ElGamal penerimalah yang harus membuat kunci publik yaitu Bella, misalkan dipilih bilangan prima $p = 2579$ dan elemen primitif $\alpha = 2$. Selanjutnya dipilih $\alpha = 765$. Maka dapat dihitung dengan rumus berikut:
  $\beta = \alpha^a \bmod p$
  $\beta = 2^{765} \bmod 2579$
  $\beta = 949$
  Sehingga diperoleh kunci publik $(p,\alpha,\beta) = (2579, 2, 949)$ dan kunci rahasia $\alpha = 765$. Kemudian Bob memberitahukan kunci publik ini kepada Alice. Dan kunci rahasia tetap dirahasiakan oleh Bob.
- ✓ Alice kemudian memperoleh kunci publik $(p,\alpha,\beta) = (2579, 2, 949)$. Dan melakukan enkripsi pesan rahasia "Perpustakaan" yang akan dikirimkannya kepada Bob.

B. Proses Enkripsi

1) Proses Enkripsi Tahap Pertama Menggunakan Vigenere Cipher
   Pesan Rahasia (Plainteks) : Perpustakaan
   Kunci : 2579,2,949

   Tabel 2. Enkripsi menggunakan Vigenere Cipher

| **Plainteks (P)** | P | e | r | p | u | s | t | a | k | a | a | n |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Indeks** | 41 | 4 | 17 | 15 | 20 | 18 | 19 | 0 | 10 | 0 | 0 | 13 |
| **Kunci (K)** | 2 | 5 | 7 | 9 | , | 2 | , | 9 | 4 | 9 | 2 | 5 |
| **Indeks** | 54 | 57 | 59 | 61 | 88 | 54 | 88 | 61 | 56 | 61 | 54 | 57 |
| **(P+K) mod 93** | 2 | 61 | 76 | 76 | 15 | 72 | 14 | 61 | 66 | 61 | 54 | 70 |
| **Ciperteks** | c | 9 | = | = | p | ( | o | 9 | # | 9 | 2 | & |

Dari Tabel 2 didapatkan hasil ciperteks dari Vigenere Cipher yaitu c9==p(o9#92&

2) Proses Enkripsi Tahap Kedua Menggunakan ElGamal

Hasil cipherteks pada Tabel 2 yang menggunakan Vigenere Cipher kemudian lakukan proses enkripsi kedua dengan menggunakan ElGamal. Dengan menggunakan pesan yang telah dienkripsi oleh Vigenere Cipher yaitu c9==p(o9#92& Kemudian terjemahkan dalam kode ASCII, seperti pada Tabel 3 ini.

Tabel 3. Konversi Pesan ke dalam Kode ASCII

| i | Karakter | Ciphertext $m_i$ (Hasil Vigenere Cipher) | ASCII |
|---|---|---|---|
| 1 | c | $m_1$ | 99 |
| 2 | 9 | $m_2$ | 57 |
| 3 | = | $m_3$ | 61 |
| 4 | = | $m_4$ | 61 |
| 5 | p | $m_5$ | 112 |
| 6 | ( | $m_6$ | 40 |
| 7 | o | $m_7$ | 111 |
| 8 | 9 | $m_8$ | 57 |
| 9 | # | $m_9$ | 35 |
| 10 | 9 | $m_{10}$ | 57 |
| 11 | 2 | $m_{11}$ | 50 |
| 12 | & | $m_{12}$ | 38 |

Berdasarkan Tabel 3 tersebut, diperoleh bahwa banyaknya karakter pada pesan tersebut adalah n = 12. Proses selanjutnya adalah menentukan bilangan acak rahasia dengan ketentuan berikut $k \in \{0,1, ..., p - 2\}$ sehigga berdasarkan p ditentukan $k_i \in \{0,1, ..., 2577\}$, dengan nilai i = 1, 2, ..., 12.

Selanjutnya berdasarkan rumus $\gamma = \alpha^k \bmod p$ dan $\delta = \beta^k .m \bmod p$, dapat dihitung nilai $\gamma_i = 2^{ki} \bmod 2579$ dan $\delta_i = 949^{ki} .m_i \bmod 2579$ seperti pada Tabel 4 dibawah ini.

Tabel 4. Proses Enkripsi menggunakan ElGamal

| i | $m_i$ | $k_i$ | $\gamma_i = 2^{ki} \bmod 2579$ | $\delta_i = 949^{ki} .m_i \bmod 2579$ |
|---|---|---|---|---|
| 1 | 99 | 1520 | 66 | 166 |
| 2 | 57 | 1843 | 1512 | 844 |
| 3 | 61 | 2183 | 1259 | 26 |
| 4 | 61 | 1606 | 2183 | 766 |
| 5 | 112 | 2210 | 838 | 970 |
| 6 | 40 | 1091 | 195 | 2451 |
| 7 | 111 | 1527 | 711 | 1808 |
| 8 | 57 | 1404 | 313 | 2211 |
| 9 | 35 | 869 | 2473 | 1561 |
| 10 | 57 | 183 | 1516 | 1007 |
| 11 | 50 | 2040 | 2099 | 992 |
| 12 | 38 | 1230 | 235 | 340 |

Berdasarkan Tabel , diperoleh ciphertext $(\gamma_i,\delta_i)$, i = 1, 2, ..., 12 sebagai berikut.

(66, 166) (1512, 844) (1259, 26) (2183, 766) (838, 970) (195, 2451)

(711, 1808) (313, 2211) (2473, 1561) (1516, 1007) (2099, 992) (235, 340)

Selanjutnya, Alice mengirim Cipherteks ini kepada Bob.

C. Proses Dekripsi

1) Proses Dekripsi Tahap Pertama menggunakan ElGamal

Pada saat Bob menerima pesan yang telah dienkripsi sebelumnya oleh si pengirim Alice, Bob harus mendekripsikan cipherteks tersebut agar bisa dibaca. Proses dekripsi dilakukan dengan menggunakan kunci yang telah Bob buat sebelumnya yaitu dengan kunci publik p = 2579 dan kunci rahasia α = 765. Dapat dilihat pada Tabel 5 dibawah ini.

Tabel 5. Proses Dekripsi menggunakan ElGamal

| i | $\delta_i$ | $\gamma_i$ | $m_i = \delta_i . \gamma_i^{1813} \bmod 2579$ | Karakter |
|---|---|---|---|---|
| 1 | 166 | 66 | 99 | c |
| 2 | 844 | 1512 | 57 | 9 |
| 3 | 26 | 1259 | 61 | = |
| 4 | 766 | 2183 | 61 | = |
| 5 | 970 | 838 | 112 | p |
| 6 | 2451 | 195 | 40 | ( |
| 7 | 1808 | 711 | 111 | o |
| 8 | 2211 | 313 | 57 | 9 |
| 9 | 1561 | 2473 | 35 | # |
| 10 | 1007 | 1516 | 57 | 9 |
| 11 | 992 | 2099 | 50 | 2 |
| 12 | 340 | 235 | 38 | & |

Dari Tabel 5 tersebut dengan menggunakan ElGamal didapatkan hasil karakter yaitu c9==p(o9#92& .

2) Proses Dekripsi Tahap Kedua menggunakan Vigenere Cipher

Kemudian dari karakter yang didapatkan sebelumnya dengan menggunakan ElGamal yaitu c9==p(o9#92& . Selanjutnya lakukan proses dekripsi tahap kedua menggunakan vigenere cipher seperti pada Tabel 6 dibawah ini.

Tabel 6. Proses Dekripsi menggunakan Vigenere Cipher

| **Cipherteks** | c | 9 | = | = | p | ( | o | 9 | # | 9 | 2 | & |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Indeks (C)** | 2 | 61 | 76 | 76 | 15 | 72 | 14 | 61 | 66 | 61 | 54 | 70 |
| **Kunci** | 2 | 5 | 7 | 9 | , | 2 | , | 9 | 4 | 9 | 2 | 5 |
| **Indeks (K)** | 54 | 57 | 59 | 61 | 88 | 54 | 88 | 61 | 56 | 61 | 54 | 57 |
| **(C-K) mod 93** | 41 | 4 | 17 | 15 | 20 | 18 | 19 | 0 | 10 | 0 | 0 | 13 |
| **Plainteks** | P | e | r | p | u | s | t | a | k | a | a | n |

Dari Tabel 6 diatas diperoleh pesan rahasia yang sebenarnya dikirimkan oleh Alice yaitu “Perpustakaan”.

## 3. Simpulan

Kombinasi penggabungan dua metode ini disebut kriptografi hibrid merupakan penggabungan antara dua kriptografi simetris dan asimetris, dimana Vigenere Cipher merupakan golongan kriptografi simetris dan ElGamal merupakan golongan kriptografi asimetris. Dalam proses pembentukan kunci dilakukan menggunakan ElGamal yang terdiri dari kunci rahasia (*private key*) dan kunci publik (*public key*). Dari penggabungan antara dua metode ini mempunyai kemampuan yang baik dalam mengatasi masalah distribusi kunci. Saat pembentukan kunci, sang penerima pesan membuat kunci publik dan kunci rahasia, kunci rahasia tetap dipegang penerima dan kunci publik diserahkan pada pengirim atau pembuat pesan. Kemudian, pesan yang akan dikirim oleh pembuat pesan mengenkripsi pesannya dengan kunci publik yang diterimanya.

Kriptografi *hybrid* memanfaatkan dua tingkatan kunci artinya proses enkripsi dan dekripsi dilakukan dua kali penguncian masing-masing. Maka dari itulah semakin aman semakin tidak nyaman, dan berlaku juga sebaliknya semakin nyaman semakin tidak aman. Kriptografi hibrid sering dipakai karena

memanfaatkan keunggulan kecepatan pemrosesan data oleh algoritma simetris dan kemudahan transfer kunci menggunakan algoritma asimetris. Hal ini mengakibatkan peningkatan kecepatan tanpa mengurangi kenyamanan serta keamanan. Dan kombinasi dua metode Vigenere Cipher dan ElGamal ini dapat digunakan dengan baik untuk keamanan pesan rahasia.

**Ucapan Terima Kasih**

Penulis mengucapkan terima kasih kepada seluruh pihak yang telah memberikan dukungan baik moril maupun materil sehingga penulis berhasil menyelesaikan paper ini dengan baik sesuai dengan harapan. Semoga paper ini dapat memberikan manfaat bagi masyarakat pada umumnya dan terkhususnya masyarakat akademik.

**Daftar Pustaka**

[1]. Mustari, M. (2010). *Aplikasi Simulasi Autentikasi Data Menggunakan Metode Schnorr Authentication Dan Digital Signature Scheme Menggunakan Metode Schnorr Authentication*. Pekanbaru: Universitas Islam Negeri Sultan Syarif Kasim Riau

[2]. Ifanto, M. (2009). *Metode Enkripsi dan Dekripsi Dengan Menggunakan Algoritma Elgamal*. Bandung: Institut Teknologi Bandung, (13508110).

[3]. Massandy, D. T. (2009). *Algoritma Elgamal Dalam Pengamanan Pesan Rahasia*. *Institut Teknologi Bandung*, 1–5. Retrieved from www.informatika.stei.itb.ac.id

[4]. Riyanto, M Zaki. (2007). *Menggunakan Algoritma Kriptografi Elgamal Atas Grup Pergandaan Zp**. Yogyakarta: Departemen Pendidikan Nasional Universitas Gadjah Mada Fakultas Matematika dan Ilmu Pengetahuan Alam.

[5]. Noercholis, A., & Asyanto, P. (2014). *Aplikasi Kriptografi Teks Pada Sms ( Short Message Service ) Dengan Menggunakan Metode Vigenere Cipher*. Sekolah Tinggi Manajemen Informatika dan Komputer ASIA Malang. *Jurnal Ilmiah Teknologi Dan Informasi ASIA*, *8*(1), 1–9.

[6]. Prabowo, H. E., & Hangga, A. (2015). *Enkripsi Data Berupa Teks Menggunakan Metode Modifikasi Vigenere Cipher*. Yogyakarta: Universitas Negeri Semarang, 1–4.

[7]. Ariyus, Dony. (2008). *Pengantar Ilmu Kriptografi (Teori, Analisis, dan Implementasi)*. Yogyakarta: ANDI Offset.

[8]. Putra, Muh Eka. (2017). *Implementasi Kombinasi Algoritma Kriptografi Metode Vigenere Cipher 5Xkey Dengan Metode Alpha-Qwerty Riverse Pada Aplikasi SMS Berbasis Android (Skripsi)*. Palembang: *Politeknik Negeri Sriwijaya*.